Sigma J Eng & Nat Sci 9 (4), 2018, 371-382

Publications Prepared for Transist 2017,
10th International İstanbul Transport Congress

Research Article

DETERMINING THE MOST VULNERABLE COMPONENTS IN A TRANSPORTATION NETWORK

Hande KÜÇÜKAYDIN[1], Necati ARAS*[2]

[1]*Dept. of Industrial Engineering, MEF University, İSTANBUL;* ORCID:0000-0003-2527-2064
[2]*Dept. of Industrial Engineering, Boğaziçi University, İSTANBUL;* ORCID:0000-0002-1485-730X

Received: 05.10.2018 Revised: 06.12.2018 Accepted: 21.12.2018

ABSTRACT

Transportation networks belong to the class of critical infrastructure networks since a small deterioration in the service provision has the potential to cause considerable negative consequences on everyday activities. Among the reasons for the deterioration we can mention the shutdown of a subway station, the closure of one or more lanes on a bridge, the operation of an airport at a much reduced capacity. In order to measure the vulnerability of transportation network, it is necessary to determine the maximum possible disruption by assuming that there is an intelligent attacker wishing to give damage to the components of the network including the stations/stops and linkages. Identifying the worst disruptions can be realized by using interdiction models that are formulated by a bilevel mathematical programming model involving two decision makers: leader and follower. In this paper, we develop such a model referred to as attacker-operator model, where the leader is a virtual attacker who wants to cause the maximum possible disruption in the transportation network by minimizing the amount of flow among the nodes of the network, while the follower is the system operator who tries to reorganize the flow in the most effective way by maximizing the flow after the disruption. The benefit of such a model to the system operator is to determine the most vulnerable stations and linkages in the transportation network on one hand, and to take precautions in preventing the negative effects of the disruption on the other hand.

Keywords: Transportation network, interdiction, bilevel programming.

1. INTRODUCTION AND BACKGROUND INFORMATION

Disruptions that can arise in the operation of a network established to provide service or products to customers (e.g., a transportation network, electric power distribution network, supply chain network, telecommunication network) may lead to serious problems in daily activities. For example, the shutdown of a subway station for access, the closure of one or more lanes on a bridge, the operation of an airport at a much reduced capacity, the disruption of an electric power plant, a damage in the power line between the power plant and customer location have the potential to result in significant drop in the quality of the provided service. Networks which are subject to considerable disruption in product and/or service provision capability are referred to as critical infrastructure networks (CINs). Formally, a network is described as a CIN when some of its components function under full capacity due to a partial damage or become fully unusable.

[*] Corresponding Author: e-mail: arasn@boun.edu.tr, tel: (212) 359 75 06

There exist two causes for the disruption in CINs: random man-made or natural causes, and intentional man-made causes. Among the random man-made causes, we can mention overlooked issues during maintenance or unintentional wrong usage. Random natural causes can be earthquake, flood, avalanche, hurricane among others. The second category is intentional man-made causes. Among these, we can name terrorist actions or other types of attacks such as cyber-attacks caused by hackers. The attacks in this last category have the potential to cause the largest damage or disruption as they do not occur randomly, but are planned by an intelligent agent. For this reason, in order to measure the vulnerability of a CIN, it is necessary to determine the maximum possible disruption by assuming that there is an intelligent attacker wishing to give damage to the system. As a matter of fact, real terrorist attacks to CINs occurred in the past had severe consequences and led to considerable loss of life and property. Examples include the attacks to a Paris subway train in 1995 and Madrid suburban trains in 2004, the bombing of London bus stops and metro stations in 2005, and the suicide attacks on two different metro stations in Moscow in 2010. Bombings to Madrid's suburban trains in 2004 severely damaged Madrid's suburban railway infrastructure with 191 people losing their lives. Partial destruction occurred in trains where bombs were blown and 114 dwellers were destroyed. As a result, Madrid's regional economy suffered losses of € 212 million [1]. An interesting study carried out by means of network analysis indicated that the metro stations in London suicide bombings were not randomly selected. Indeed, the three stations selected were the ones closest to the best location among three million possible combinations to choose [2]. March 2016 witnessed three coordinated suicide bombings in Belgium: two at Brussels Airport and one at a metro station. Following the attack, all departure flights were suspended but the arrival flights remained operational for some time until they were diverted. In June 2016, Atatürk Airport in İstanbul was the scene to a terrorist attack with shootings and suicide bombings. Most of the İstanbul-bound flights were diverted to other major airports in Turkey, and Federal Aviation Administration suspended all flights from Turkey into United States and from United States into Turkey for about five hours with the exception of 10 flights that were airborne during the attack with a destination in United States. More recently, in April 2017, the overall subway system of St. Petersburg was closed for several hours as the consequence of an explosion in one of the metro stations. Note that St. Petersburg's subway system carries 2 million passengers per day.

In the operations research literature, the vulnerability of CINs is analyzed by developing reliability models when the factors giving rise to disruptions are random man-made or natural causes. On the other hand, as stated in Smith [3] analyzing the worst disruptions is dealt with using interdiction models that are generally formulated by a bilevel mathematical program which corresponds to a Stackelberg game with two decision makers. Note that classical single-level optimization models only involve a single decision maker. The two decision makers in a Stackelberg game are referred to as the leader and the follower. Each of them has control over its own decision variables, constraints, and objective functions. In some cases, the objective functions turn out to be the same, but the sense of optimization is different. Namely, one player wants to minimize its objective function, whereas the other maximizes exactly the same function. A bilevel mathematical model is formulated from the perspective of the leader, and the optimization problem of the follower referred to as the lower-level problem (LLP) is incorporated into the leader’s upper-level problem (ULP). In other words, the leader solves her own optimization problem by taking into account the optimal reaction of the follower to her decisions.

There exist two streams of research within the context of interdiction problems. The first stream focuses on facility interdiction problems, while the second one addresses network interdiction problems. In the former problem, the targets of the attacker are facilities that provide service to customers. The first facility interdiction models in the literature are based on the work of Church et al. [4] where the authors are concerned with both median-type and coverage-type location problems, and introduce a model for each type from the perspective of the attacker. The *r*-interdiction median problem involves the maximization of the demand-weighted total distance by destroying *r* out of *p* facilities as a result of which, customers of the interdicted facilities need to be reassigned to operating facilities to get service. The *r*-interdiction covering problem, on the other hand, consists of determining a subset of *r* facilities among the set of *p* existing ones so that their destruction yields the largest reduction in covered customer demand. It is worth emphasizing that these two problems are the opposite of the well-known *p*-median and maximal covering location problems.

In network interdiction models, the interdicted components become the edges or arcs of the network. The system operator tries to find the shortest path between an origin-destination node pair or the maximum flow from an origin node to a destination node given that some of these arcs are completely or partially damaged by an attacker. The problem of the attacker is then to determine the arcs to interdict so as to maximize the shortest path or minimize the maximum flow. The network interdiction models have been investigated for a longer period in the literature. The first study [5] examines the minimization of the maximum possible flow between an origin-destination pair in a network by interdicting a predetermined number of arcs and making them unusable. Later, Wood [6] addresses the same problem with the possibility of both complete and partial interdiction of arcs under a budget constraint for the attacks. Cormican et al. [7] consider a variant of this problem where the attacks bring about disruption with a certain probability. In that study, the objective function of the attacker is minimization of the maximum flow under the restriction that arcs of the network are destroyed with probability $1-p$ according to a Bernoulli process. The shortest path network interdiction problem in which the lengths of the arcs are increased as a result of attacks is presented in the literature for the first time by Fulkerson and Harding [8]. Later on, Israeli and Wood [9] study the same problem under the assumption that arcs are completely destructed by the attacker. Lim and Smith [10] apply the same idea to a multi-commodity network flow problem where the capacity of each arc is partially or completely reduced.

In this paper, a bilevel attacker-operator model is developed for a transportation network where the leader is an intelligent virtual attacker who wants to cause the largest disruption in the flow amount of passengers traveling among the nodes of the network by damaging the stations and/or linkages. The follower, on the other hand, is the system operator who tries to reorganize the flow on the network in the most effective way so as to maximize the passenger flow after the disruptions caused by the attacker. Recall that the virtual attacker is just a proxy for determining the most significant stations and linkages in terms of the vulnerability of the transportation network. If this intelligent virtual attacker were not considered as a decision maker, then it could not be possible to determine the most vulnerable components of the transportation network.

An important distinction between the attacker-operator models in the literature and the one proposed in this study is that both nodes and arcs may be attacked. Note that a node in the transportation network corresponds to a station/stop, whereas an arc corresponds to a linkage between two stations. The attacks on stations as well as linkages can be carried out in such a way that partial disruption is possible. If a component is completely interdicted, then it becomes unusable and cannot provide any service. However, a component that is partially interdicted continues to provide service at a reduced capacity. A complete interdiction assumption that is frequently used in the literature makes the mathematical programming formulation easy to solve, but it does not reveal potential situations that can be encountered in real life. In many cases, both nodes and arcs continue to serve at a reduced capacity rather than being fully inoperable. An example for this would be the drop in the number of vehicles serving between two stations due to the reduction of the linkage capacity after an attack. Such a case cannot be handled correctly with a model taking into account only complete interdictions. The model developed in this paper is flexible enough to incorporate both a partial interdiction and a complete interdiction. We develop the model for the former case, and but it is straightforward to change it for the latter case.

The remainder of the paper is organized as follows. Section 2 presents the bilevel mathematical model that is developed. Section 3 includes the solution method with all the necessary details. Experimental results are given in Section 4, while the paper is concluded in Section 5.

2. BILEVEL MATHEMATICAL MODEL

As mentioned earlier, interdiction models are represented as bilevel mathematical programs which correspond to a Stackelberg game studied in game theory [11]. Such a game involves two players: the leader and the follower. These players make their decisions sequentially, namely the leader moves first and makes a decision that is observed by the follower who reacts to the leader by making her own decision. Two important assumptions are also made frequently: (i) both players are rational decision makers meaning that they want to make the best decision available to them, (ii) the follower's optimization problem, i.e., the LLP is known to the leader. As a consequence, we can interpret a Stackelberg game from the perspective of the leader as follows: the LLP of the follower is incorporated into the constraints of the leader so that the leader takes the LLP into account while determining the optimal solution of her own problem. A bilevel mathematical model can generally be represented as follows:

$$\begin{aligned}
&\min_{\mathbf{x}} F(\mathbf{x},\mathbf{y}) \\
&\text{subject to} \quad G_i(\mathbf{x},\mathbf{y}) \le 0 \\
&\qquad \min_{\mathbf{y}} f(\mathbf{x},\mathbf{y}) \\
&\qquad \text{subject to } g_i(\mathbf{x},\mathbf{y}) \le 0
\end{aligned}$$

In this formulation, **x** and **y** stand for the leader's and follower's decision variables, respectively. $F(\mathbf{x},\mathbf{y})$ represents the objective function in the ULP (i.e., leader's objective function), while $f(\mathbf{x},\mathbf{y})$ is the objective function in the LLP (i.e., follower's objective function). Similarly, $G_i(\mathbf{x},\mathbf{y}) \le 0$ and $g_i(\mathbf{x},\mathbf{y}) \le 0$ indicate the *i*th constraint of the leader and the follower, respectively. In general, bilevel programs are more difficult to solve than traditional single-level programs. The easiest bilevel programs are the ones where both the ULP and LLP are linear programs. It was shown by Jeroslow [12] that even these problems are NP-hard. The difficulty level and the choice of the solution method of bilevel programs depend on the existence of integer decision variables in the LLP. If there exist only continuous decision variables in the LLP, and the LLP is a convex minimization or concave maximization problem, then it becomes possible to reduce the bilevel formulation into a single-level one by writing the Karush-Kuhn-Tucker (KKT) optimality conditions for the LLP and adding them into the ULP. However, the resulting equivalent single-level formulation is nonlinear due to the complementary slackness constraints obtained as a consequence of KKT optimality conditions of the LLP. Therefore, the exact solution of the single-level formulation requires in general the application of global optimization techniques. However, as can be seen in the sequel, these nonlinear constraints can be converted to linear ones by means of appropriate linearization techniques [13].

The problem considered in this paper is referred to as the Attacker-Operator Problem with Partial Interdiction (AOP-PI). Recall that the motivation of this study is to determine the most vulnerable components in a transportation network which helps the system authorities to find answer to the following question: which stations and linkages are critical in the sense that the passenger flow in the network is affected the most when there is a disruption of the service due to an attack to these stations and linkages? Below, we first provide the index sets, parameters, and decision variables that are used in the definition of the AOP-PI, and then we give the bilevel programming formulation of the considered problem.

Index sets:

$i \in N$: stations in the network
$b \in B \subseteq N$: stations in the network at which passenger flow begins (origins)
$s \in S \subseteq N$: stations in the network at which passenger flow ends (destinations)
$(b,s) \in T$: station pairs between which there is a passenger flow (origin-destination pairs)
$j \in A$: linkages in the network
$k \in K_{bs}$: admissible paths that connect origin station *b* to destination station *s*

Parameters:

f_{bs} : number of passengers willing to travel from origin *b* to destination *s*
d_i : the maximum throughput of passengers at station *i*
e_j : the maximum throughput of passengers at linkage *j*
o_i : amount of resource required for complete interdiction of station *i*
p_j : amount of resource required for complete interdiction of linkage *j*
r : the amount of resource available to the attacker for interdiction
α_{bs}^{ki} : indicator parameter taking value 1 if admissible path *k* from origin station *b* to destination station *s* includes station *i*, 0 otherwise
β_{bs}^{kj} : indicator parameter taking value 1 if admissible path *k* from origin station *b* to destination station *s* includes linkage *j*, 0 otherwise

Decision variables:

$0 \le X_i \le 1$: Interdiction level at station *i*
$0 \le Y_j \le 1$: Interdiction level at linkage *j*
Z_{bsk} : Number of passengers who can commute between origin *b* and destination *s* on admissible path *k* after the disruption

$$\min_{\mathbf{X},\mathbf{Y}} \sum_{(b,s)\in T} \sum_{k\in K_{bs}} Z_{bsk} \tag{1}$$

$$\text{subject to} \quad \sum_{i\in N} o_i X_i + \sum_{j\in N} p_j Y_j \le r \tag{2}$$

$$0 \le X_i \le 1 \quad i \in N \tag{3}$$

$$0 \le Y_j \le 1 \quad j \in N \tag{4}$$

$$\max_{\mathbf{Z}} \sum_{(b,s)\in T} \sum_{k\in K_{bs}} Z_{bsk} \tag{5}$$

$$\text{subject to} \quad \sum_{(b,s)\in T} \sum_{k\in K_{bs}} \alpha_{bs}^{ki} Z_{bsk} \le d_i(1-X_i) \qquad i \in N \tag{6}$$

$$\sum_{(b,s)\in T} \sum_{k\in K_{bs}} \beta_{bs}^{kj} Z_{bsk} \le e_j(1-Y_j) \qquad j \in A \tag{7}$$

$$\sum_{k\in K_{bs}} Z_{bsk} \le f_{bs} \quad b \in B, s \in S \tag{8}$$

$$Z_{bsk} \ge 0 \qquad b \in B, s \in S, k \in K_{bs} \tag{9}$$

In this model, (1)–(4) represent the ULP while (5)–(9) indicate the LLP. Expression (1) denotes the objective function of the ULP which is to be minimized by the virtual attacker. This function counts the number of passengers who can travel among all origin-destination pairs over all admissible paths after the disruption. Note that the system planner, who is the follower in the bilevel program, tries to maximize the same objective function with expression (5). Here, an admissible path K_{bs} designates a path on which the duration of travel from origin *b* to destination *s* takes less than a threshold value. In other words, if traveling time from *b* to *s* on path K_{bs} after the disruption takes longer than a certain amount acceptable by the passengers, then that path is not used anymore for commuting purposes. Constraint set (2) ensures that the total amount of resource used by the attacker for interdicting stations and linkages does not exceed the available amount *r*. Constraints (3) and (4) show the values of the attacker's decision variables. Notice that an upper limit of one corresponds to the case of complete interdiction, whereas a fractional value less than one indicates partial interdiction.

The constraints of the LLP, which is the optimization problem of the system planner, are given by expressions (6)–(9). Specifically, constraint set (6) ensures that the total passenger flow through station *i* does not exceed its capacity after the interdiction. In a similar fashion, constraint set (7) guarantees that the total passenger flow through linkage *j* is limited by the capacity of that linkage following the interdiction. Constraints (8) set an upper limit for the total number of passengers traveling over all admissible paths connecting origin-destination pairs. Finally, constraint set (9) are the nonnegativity restrictions on number of passengers who can commute between origin *b* and destination *s* on admissible path *k* after the disruption.

3. SOLUTION METHOD

In the bilevel AOP-PI, the LLP of the follower is a linear program. As alluded to earlier, since the LLP contains only continuous decision variables (i.e., Z_{bsk}), it is possible to write the KKT optimality conditions of the LLP and incorporate them to the ULP of the leader so as to obtain a single-level nonlinear program. The KKT conditions require to define KKT multipliers for the constraints (6)–(9) in the LLP. By introducing λ_i for constraints (6), μ_j for constraints (7), γ_{bs} for constraints (8), and θ_{bsk} for constraints (9), and converting constraints (6)–(9) to equalities by defining slack variables Δ_{1i}, Δ_{2j}, Δ_{3bs}, and Δ_{4bsk}, the following KKT conditions can be written:

Primal feasibility constraints:

$$\sum_{b\in N}\sum_{s\in N}\sum_{k\in K_{bs}} \alpha_{bs}^{ki} Z_{bsk} + \Delta_{1i} = d_i(1-X_i) \quad i \in N \tag{6'}$$

$$\sum_{b\in N}\sum_{s\in N}\sum_{k\in K_{bs}} \beta_{bs}^{kj} Z_{bsk} + \Delta_{2j} = e_j(1-Y_j) \quad j \in A \tag{7'}$$

$$\sum_{k\in K_{bs}} Z_{bsk} + \Delta_{3bs} = f_{bs} \qquad b \in B, s \in S \tag{8'}$$

$$-Z_{bsk} + \Delta_{4bsk} = 0 \qquad b \in B, s \in S, k \in K_{bs} \tag{9'}$$

Dual feasibility constraints:

$$\lambda_i \geq 0 \quad i \in N \tag{10}$$

$$\mu_j \geq 0 \quad j \in A \tag{11}$$

$$\gamma_{bs} \geq 0 \quad b \in B, s \in S \tag{12}$$

$$\theta_{bsk} \geq 0 \qquad b \in B, s \in S, k \in K_{bs} \tag{13}$$

Complementary slackness constraints:

$$\lambda_i \Delta_{1i} = 0 \quad i \in N \tag{14}$$

$$\mu_j \Delta_{2j} = 0 \quad j \in A \tag{15}$$

$$\gamma_{bs}\Delta_{3bs} = 0 \quad b \in B, s \in S \tag{16}$$

$$\theta_{bsk}\Delta_{4bsk} = 0 \qquad b \in B, s \in S, k \in K_{bs} \tag{17}$$

Stationarity constraint: $1 - \sum_i \lambda_i \alpha_{bs}^{ki} - \sum_j \mu_j \beta_{bs}^{kj} - \gamma_{bs} + \theta_{bsk} = 0 \;\; b \in B, s \in S, k \in K_{bs}$ (18)

Notice that constraints (14)–(17) are nonlinear since they involve the multiplication of two decision variables, namely KKT multipliers and slack variables. Fortunately, these nonlinear constraints can be linearized by defining for each constraint binary variables U_{1i} , U_{2j} , U_{3bs} , and U_{4bsk} and using parameter *M* that constitutes an upper bound on the slack variables. As a result, the following linear constraints can be written:

$$\lambda_i - MU_{1i} \le 0 \tag{14'}$$

$$\Delta_{1i} - M(1 - U_{1i}) \le 0 \tag{14"}$$

$$\mu_j - MU_{2j} \le 0 \tag{15'}$$

$$\Delta_{2j} - M(1 - U_{2j}) \le 0 \tag{15"}$$

$$\gamma_{bs} - MU_{3bs} \le 0 \tag{16'}$$

$$\Delta_{3bs} - M(1 - U_{3bs}) \le 0 \tag{16"}$$

$$\theta_{bsk} - MU_{4bsk} \le 0 \tag{17'}$$

$$\Delta_{4bsk} - M(1 - U_{4bsk}) \le 0 \tag{17"}$$

Finally, a single-level mixed-integer linear programming model is obtained which has the objective of minimizing $\sum_{(b,s)\in T}\sum_{k\in K_{bs}} Z_{bsk}$ subject to constraints (2)–(4), (6')–(9'), (10)–(13), (14')–(18).

4. EXPERIMENTAL RESULTS

In this section, the resulting single-level model for the AOP-PI is solved on a simplified transportation network displayed in Figure 1 that is obtained by sampling from the Metropolitan City of İstanbul. The transport linkages are metro, metrobus, tram, and funicular line segments. The model is solved by means of Cplex 12.7.1 available within GAMS platform v24.9.

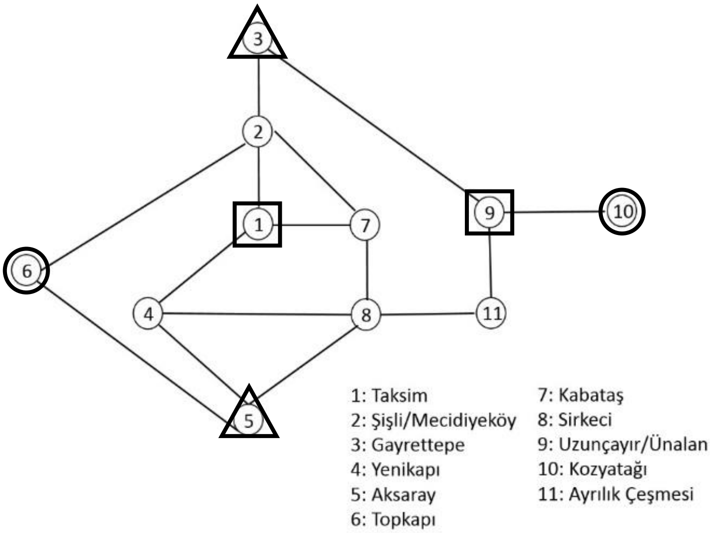

Figure 1. Simplified Transportation Network

Six stations pairs have been selected randomly as origin-destination pairs in the sample network. These are Topkapı-Kozyatağı, Kozyatağı-Topkapı (stations shown by a circle), Taksim-Uzunçayır, Uzunçayır-Taksim (stations shown by a square), Gayrettepe-Aksaray and Aksaray-Gayrettepe (stations shown by a triangle) stations. The admissible paths connecting these station pairs are given in Table 1. As can be seen, a single admissible path can be used by passengers between pairs (6,10), (10,6), (1,9), and (9,1), whereas two paths are available for pairs (3,5) and (5,3). Note that some of the paths existing between origin-destination pairs are ignored because they do not turn out to be admissible due to the fact that the commuting time on the path takes longer than a threshold duration acceptable by the passengers. For example, the paths 6-5-8-11-9-10 and 1-7-8-11-9 for origin-destination pairs (6,10) and (1,9), respectively are not admissible, and therefore are not shown in Table 1. The number of passengers willing to travel between the station pairs are as follows: $f_{6,10}$=200, $f_{10,6}$=300, $f_{1,9}$=150, $f_{9,1}$=200, $f_{3,5}$=350, $f_{5,3}$=150. We can see that the total number of passengers willing to travel in the network is equal to 1350. The maximum throughput of passengers at station i and linkage j are set to d_i = 1350 and e_j = 1350 so that all transport demand is satisfied in the network when there is no interdiction. The resource requirement for the complete interdiction of tram and metrobus stations and linkages is determined as o_i = 1 and p_j = 1. The same quantity for complete interdiction of funicular and metro stations and linkages is set to o_i = 2 and p_j = 2. The amount of resource available to the attacker for interdiction is taken as r = 2 initially, but it will be changed in further experiments.

Table 1. Admissible Paths for Station Pairs

Station pair	Path 1	Path 2
(6,10)	6-2-3-9-10	–
(10,6)	10-9-3-2-6	–
(1,9)	1-2-3-9	–
(9,1)	9-3-2-1	–
(3,5)	3-2-6-5	3-2-1-4-5
(5,3)	5-6-2-3	5-4-1-2-3

When the problem is solved, it is seen that the best alternative for the attacker is to interdict the third station (Gayrettepe station). When the attacker uses its total available resource *r*=2 to completely destroy this station, the number of passengers traveling in the network drops to zero. Indeed, a close inspection of Figure 1 explains this outcome: Gayrettepe station lies on all admissible paths connecting the origin-destination pairs. When the available resource of the attacker is reduced to *r*=1, the best option becomes to completely destroy station 9 (Uzunçayır station), which brings the number of passengers down to 500 from the value of 1350. We would like to remind that the cost of complete interdiction of Uzunçayır station is o_9=1. Results obtained for other *r* values are shown in Table 2. The notation $(3,5)^1$ and $(3,5)^2$ in this table indicates the admissible path that is used between these two stations. When the results are scrutinized closely, two important observations can be made. First, the interdiction resource is consumed fully by the attacker, and second the only interdicted components of the network are stations.

Table 2. Results obtained for different values of the available resource for interdiction

Available resource for the attack	Attack level on the stations	Passenger Flow
2	X_3=1	Total=0
1.5	X_3=0.75	$(5,3)^1$=150; (6,10)=187.5 Total=337.5
1	X_9=1	$(3,5)^1$=350; $(5,3)^1$=150 Total=500

0.8	X_9=0.8	(1,9)=150; $(3,5)^2$=350; $(5,3)^2$=150;
		(6,10)=120
		Total=770

0.5	X_3=0.25	(1,9)=150; (9,1)=200;$(3,5)^1$=12.5 $(5,3)^1$=150; (6,10)=200; (10,6)=300 Total=1012.5

In order to investigate the effect of the number of admissible paths between origin-destination station pairs, we introduce another admissible path to station pairs (6,10) and (10,6) so that these two pairs have two admissible paths just as station pairs (3,5) and (5,3) do. Specifically, we add path (6-5-8-11-9-10) for pair (6,10) and path (10-9-11-8-5-6) for pair (10,6). The results obtained for the network after the addition of these paths are presented in Table 3. As can be seen, there is a change in the results compared with those provided in Table 2. Namely, the observation that the interdiction resource is consumed fully by the attacker is violated this time for the case with *r*=1.5. Note that only one unit of interdiction resource is used by the attacker to interdict station 9 with 0.5 units of resource left over. At this point, a question may arise as to why this amount is not used for the interdiction of the linkages on the first admissible path between station pairs (3,5) and (5,3). The reason lies in the fact that the amount of resource required for the complete interdiction of these linkages is p_j=1 and with the remaining resource of 0.5 units the amount of passenger flow can be reduced to $0.5 \times 1350 = 675$ as the original throughput capacity of passenger flow is e_j=1350. Since the current passenger flow is 350 on the first admissible path between pair (3,5), and 150 on the first admissible path between pair (5,3), and these values are already lower than 675, it is obvious that an attack to the linkages will not decrease the amount of passenger flow further.

Table 3. Results obtained when a second admissible path is added for station pairs (6,10) and (10,6)

Available resource for the attack	Attack level on the stations	Passenger Flow
2	X_5=1, X_9=1	Total=0
1.5	X_9=1	$(3,5)^1$=350; $(5,3)^1$=150 Total=500
1	X_9=1	$(3,5)^1$=350; $(5,3)^1$=150 Total=500

0.8	X_9=0.8	(1,9)=70; $(3,5)^2$=350; $(5,3)^2$=150;
		(6,10)=200
		Total=770

0.5	X_9=0.5	(1,9)=150; (9,1)=200;$(3,5)^1$=350 $(5,3)^1$=150; $(6,10)^2$=25; $(10,6)^2$=300 Total=1175

In order to identify situations in which linkages in the network are also attacked, we make a modification in one of the model parameters. The resource amount for the complete interdiction of the linkage (3,2) connecting station 3 to station 2 is set to p=0.66. Recall that its original value was equal to one. Now, the model is solved again for the case with r=1.5, and the result presented in Table 4 is obtained.

Table 4. Result obtained when the resource amount for complete interdiction of linkage (3,2) is set to p=0.66

Available resource for the attack	Attack level on the stations	Passenger Flow
1.5	X_9=0.84,$Y_{(3,2)}$=1	(1,9)=16, $(5,3)^1$=150, $(6,10)^1$=200 Total=366

We would like to point out that the required computation time of solving the model depends on several factors. They can be listed as the size of the transportation network in terms of the number of existing stations and linkages in the network, the number of admissible paths between each origin-destination station pair, and the number of nodes and linkages found on admissible paths. In order to see the effect of these factors we performed additional experiments, and observed that although an increase in each of these quantities results in an increase in the solution time, Cplex can still find the optimal solution within minutes. For example, we could find an optimal solution for instances that have a network size of 50 nodes, 5–10 origin-destination station pairs, and several admissible paths between each origin-destination pair.

5. CONCLUSIONS

In this paper, we address the problem of determining the most vulnerable components of a transportation network by using a bilevel modelling framework. This framework allows us to formulate the problem as a Stackelberg game between two players: an intelligent virtual attacker who is the leader of the game and a system operator who is the follower. The assumption of an intelligent attacker helps to find the largest disruption and hence the vulnerabilities in the transportation network. In order to incorporate the disruption of the network components as realistically as possible, a partial interdiction model is developed where a station or a linkage is not rendered necessarily out of service when interdicted, but their throughput capacity is reduced to a certain extent depending on the effort of the attacker. With the aim of exactly solving the resulting bilevel program, it is converted to a single-level model by writing the Karush-Kuhn-

Tucker conditions of the lower level problem, adding them to the upper level problem, and linearizing the nonlinear constraints arising from the complementary slackness constraints of Karush-Kuhn-Tucker conditions. The mixed-integer linear model is solved using Cplex 12.7.1 that is a state-of-the-art solver available within GAMS v24.9 modeling platform.

Future research possibilities include the following directions. First, the same bilevel model can be employed for the case complete interdiction of the network components with a small change of the definition of decicion variables **X** and **Y**. Namely, instead of representing the interdiction level at stations and linkages, they can be re-defined so that that they denote whether the stations and linkages are destroyed or not. This implies that a station or linkage is damaged completely when attacked. A comparison of the results obtained by partial interdiction and complete interdiction models may provide further insight on the nature of the network vulnerability. Second, another level can be added to the problem to include the protection decision of the system planner, which gives rise to a trilevel operator-attacker-operator problem. The solution of this model can yield hints with regard to the actions to increase the resilience of the transportation network. Lastly, the interdiction decision of the attacker in the attacker-operator model considered in this paper and the protection decision of the operator in the aforementioned trilevel model can be given in a dynamic fashion within a planning horizon, which necessitates a multi-period models.

Acknowledgements

This work is partially supported by grant no. 117M593 received from The Scientific and Technological Research Council of Turkey.

REFERENCES

[1] Buesa M., Valiňo A., Heijs J., Baumert T., González Gomez J., 2004, "The Economic Cost of March 11: Measuring the Direct Economic Cost of the Terrorist Attack on March 11, 2004 in Madrid", Working paper no. 54, Instituto de Análisis Industrial y Financiero. Universidad Complutense de Madrid.

[2] Jordán F., (2008) Predicting target selection by terrorists: a network analysis of the 2005 London underground attacks, *International Journal of Infrastructures* 4(1/2), 206–214.

[3] Smith J.C., 2010, "Basic interdiction models", in Cochran J. (Ed.), Wiley Encyclopedia of Operations Research and Management Science, Wiley, New York.

[4] Church R.L., Scaparra M.P., Middleton R.S., (2004) Identifying Critical Infrastructure: the Median and Covering Facility Interdiction Problems, *Annals of the Association of American Geographers* 94(3), 491–502.

[5] Wollmer R., (1964) Removing arcs from a network, *Operations Research* 12(6), 934–940.

[6] Wood R.K., (1993) Deterministic network interdiction, *Mathematical and Computer Modelling* 17(2), 1–18.

[7] Cormican K.J., Morton D.P., Wood, R.K, (1998) Stochastic Network Interdiction, *Operations Research* 46(2), 184–197.

[8] Fulkerson D.R., Harding G.C., (1977) Maximizing the minimum source-sink path subject to a budget constraint, *Mathematical Programming* 13(1), 116–118.

[9] Israeli E., Wood R.K., (2002) Shortest-path network interdiction, *Networks* 40(2), 97–111.

[10] Lim C., Smith J.C., (2007) Algorithms for discrete and continuous multicommodity flow network interdiction problems, *IIE Transactions* 39(1), 15–26.

[11] von Stackelberg, H. 1952. The Theory of Market Economy. New York: Oxford University Press.

[12] Jeroslow R.G., (1985) The polynomial hierarchy and a simple model for competitive analysis, *Mathematical Programming* 32(2), 146–164.

[13] Grossmann I.E., Floudas C.A., (1987) Active constraint strategy for flexibility analysis in chemical processes, *Computers and Chemical Engineering*, 11(6), 675–693.